FINITE FIELDS AND THEIR APPLICATIONS **3,** 131–139 (1997)
ARTICLE NO. FF960174

The Existence of a Self-Dual [70, 35, 12] Code and Formally Self-Dual Codes

Masaaki Harada

Department of Mathematics, Okayama University, Okayama 700, Japan

Received December 28, 1995; revised August 8, 1996

In this note, the existence of self-dual codes and formally self-dual even codes is investigated. A construction for self-dual codes is presented, based on extending generator matrices. Using this method, a singly-even self-dual [70, 35, 12] code is constructed from a self-dual code of length 68. This is the first published example of a singly-even [70, 35, 12] code. Constructions are also given for formally self-dual even codes. Extremal formally self-dual even codes are constructed. © 1997 Academic Press

1. INTRODUCTION

An $[n, k]$ linear code C over $GF(q)$ is a k-dimensional vector subspace of $GF(q)^n$, where $GF(q)$ is the Galois field of q elements. The elements of C are called codewords and the weight of a codeword is the number of nonzero coordinates. An $[n, k, d]$ code is an $[n, k]$ code with minimum (nonzero) weight d. Two codes C and C' are equivalent if there exists a monomial matrix M over $GF(q)$ such that $C' = CM$. The weight enumerator $W_C(y)$ of a code C is given by $W_C(y) = \sum_{i=0}^{n} A_i y^i$, where A_i is the number of codewords of weight i in C. The numbers $A_0, \ldots, A_n$ are called the weight distribution of C.

The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in GF(q)^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. A code C is *self-dual* if $C = C^\perp$. A code C is *formally self-dual* if the codes C and $C^\perp$ have identical weight distributions. Self-dual codes are formally self-dual, but there are formally self-dual codes which are not self-dual. A formally self-dual code is *divisible* if there exists a positive integer $\delta > 1$ such that δ divides all the nonzero weights in the code. The most

1071-5797/97 $25.00

interesting self-dual codes or formally self-dual codes are divisible. The Gleason–Pierce theorem characterizes the fields for which there exists a formally self-dual divisible code.

THEOREM 1 (Gleason–Pierce). *Suppose C is a formally self-dual divisible code over $GF(q)$. Then one of the following holds*:

Type I: $q = 2$ *and* $\delta = 2$,

Type II: $q = 2$ *and* $\delta = 4$,

Type III: $q = 3$ *and* $\delta = 3$,

Type IV: $q = 4$ *and* $\delta = 2$ *or*

Type V: *a repetition code over any field.*

The trivial Type V codes are not considered in this note. For Types II, III, and IV, a formally self-dual divisible code is also self-dual (cf. [5]). In this note, the existence of Type I self-dual codes and Type I formally self-dual codes is investigated. Self-dual codes of Type I are called *singly-even self-dual* and self-dual codes of Type II are called *doubly-even self-dual*. Formally self-dual codes of Type I are called *formally self-dual even* (cf. [5]). The minimum weight d of a Type I code of length $2n$ is bounded by $d \leq 2[n/4] + 2$. A formally self-dual even $[2n, n, d]$ code with $d = 2[n/4] + 2$ is called *extremal*. For $2n = 32, 40, 42, 48, 50, 52$ and $n \geq 56$, the weight enumerator of an extremal formally self-dual even code contains a negative coefficient (cf. [10]). Thus there cannot exist an extremal formally self-dual even code for these lengths. For self-dual codes, Ward [15] proved that there exist extremal singly-even self-dual codes for lengths 2, 4, 6, 8, 12, 14, 22, 24 and for no other length. Recently, Conway and Sloane [3] obtained an improved upper bound for the minimum weight of singly-even self-dual codes by considering the weight enumerators of the shadows. They also determined the largest possible minimum weight for self-dual codes of length up to 72. A self-dual code is *extremal* if it has the largest minimum weight for that length.

A symmetric 2-(v, k, λ) design D is an incidence structure consisting of v points and v blocks with the property that any block is incident with k points and any two blocks are incident with exactly λ common points. This note considers only nontrival symmetric designs. A design D can be represented by its incidence matrix $M = (m_{ij})$, where $m_{ij} = 1$ if the ith point is incident with the jth block and $m_{ij} = 0$ otherwise. Two symmetric designs are isomorphic if the incidence matrix of one design can be obtained from the incidence matrix of another by permuting its rows and columns. A design obtained by interchanging the roles of points and blocks of a design D is called the dual design of D. A symmetric design is *self-dual* if the dual design and the initial design are isomorphic.

In this note, the existence of self-dual codes and formally self-dual even codes is investigated. In Section 2, a construction is presented for self-dual codes based on extending generator matrices. Using this method, a singly-even [70, 35, 12] code is constructed from a self-dual code of length 68. This code is the first published example of a singly-even self-dual [70, 35, 12] code. Section 3 presents constructions of formally self-dual even codes. Extremal formally self-dual even codes are constructed. The notation and terminology follow that in [9] for coding theory and [13] for symmetric designs.

2. CONSTRUCTION OF A SINGLY-EVEN [70, 35, 12] CODE

All codes considered in this section are self-dual codes. Conway and Sloane [3] determined the largest possible minimum weight for length $2n \leq 72$ by considering the weight enumerators of shadows. The possible weight enumerators for extremal self-dual codes of length $2n \leq 64$ and $2n = 72$ were given in [3]. From Theorem 5 in [3], one can easily determine the possible weight enumerators for length $n \geq 66$. According to Table I in [3], the largest possible minimum weight for length 70 is 12; however, it is easy to see that this is 14, considering the possible weight enumerators of a singly-even [70, 35, 14] code and its shadow. The possible weight enumerators for an extremal singly-even [70, 35, 14] code and its shadow code were first computed in [6]. Unfortunately, the weight enumerator of the shadow was incorrectly reported. The corrected weight enumerator was given in [4].

The possible weight enumerators W and S of a singly-even self-dual [70, 35, 12] code and its shadow are of the form

$$\begin{aligned} W &= 1 + 2\beta y^{12} + (11730 - 2\beta - 128\gamma)y^{14} + (150535 - 22\beta \\ &\quad + 896\gamma)y^{16} + \cdots, \\ S &= \gamma y^7 + (\beta - 14\gamma)y^{11} + \cdots; \text{ or} \end{aligned} \tag{1}$$

$$\begin{aligned} W &= 1 + 2\beta y^{12} + (9682 - 2\beta)y^{14} + (173063 - 22\beta)y^{16} + \cdots, \\ S &= y^3 + (\beta - 104)y^{11} + \cdots, \end{aligned} \tag{2}$$

where β and γ are undetermined parameters. The weight enumerators (1) with $\beta = \gamma = 0$ coincide with the putative weight enumerators of an extremal singly-even [70, 35, 14] code and its shadow. Using the following construction, a singly-even [70, 35, 12] code is found with weight enumerator (1), $\beta = 416$ and $\gamma = 1$.

TABLE 1
The Weight Distribution of the [70, 35, 12] Code C_{70}

Weight	Frequency
0	1
12	832
14	10770
16	142279
18	1353320
20	9437352
22	49957193
24	204165154
26	650426976
28	1627816992
30	3221537516
32	5066102223
34	6348918576
36	6348918576
38	5066102223
40	3221537516
42	1627816992
44	650426976
46	204165154
48	49957193
50	9437352
52	1353320
54	142279
56	10770
58	832
70	1

PROPOSITION 2. *Let Ω be a subset of the set $\{1, 2, \ldots, n\}$ such that $|\Omega|$ is odd if $2n \equiv 0 \pmod 4$ and $|\Omega|$ is even if $2n \equiv 2 \pmod 4$. Let $G = [I_n, A]$ be a generator matrix of a self-dual code C of length $2n$, where I_n is the identity matrix of order n. Then the following matrix*

$$G^* = \begin{bmatrix} 1 & 0 & x_1 & \cdots & x_n & 1 & \cdots & 1 \\ y_1 & y_1 & & & & & & \\ \vdots & \vdots & & & & & & \\ \vdots & \vdots & & I_n & & & A & \\ & & & & & & & \\ y_n & y_n & & & & & & \end{bmatrix},$$

where $x_i = 1$ if $i \in \Omega$ and $x_i = 0$ otherwise and $y_i = x_i + 1$ $(1 \le i \le n)$, generates a self-dual code C^* of length $2n + 2$.

Proof. Since G generates a self-dual code, it is sufficient to show the orthogonalities of the first row and other rows of G^*. Let r_i be the ith row of G^*. For $2 \leq i \leq n+1$, we have

$$r_1 \cdot r_i = (x_{i-1} + 1) + x_{i-1} + k_{i-1} \equiv 0 \pmod 2,$$

where k_i is the number of 1's in the ith row of A. Therefore G^* generates a self-dual code of length $2n + 2$. ■

Remark. Brualdi and Pless [2] considered extensions of self-dual codes using the concept of shadows. These constructions were improved by Tsai [14]. We can choose the vector $(x_1, \ldots, x_n, 1, \ldots, 1)$ of length $2n$ and a fixed ith row of G with $i \notin \Omega$ as s and $\bar{s}$, respectively, in Theorem in [14]. Let C_0 be the subcode of codimension 1 of C consisting of all codewords orthogonal to $\bar{s}$. Then the above self-dual code C^* is equivalent to a self-dual code constructed from C and its shadow with respect to C_0 by the theorem in [14].

A singly-even [70, 35, 12] code is now constructed using Proposition 2. The code $D17$ in [3] is an extremal singly-even code of length 68. Starting with $D17$, many self-dual codes of length 70 can be constructed using Proposition 2. Then a singly-even self-dual [70, 35, 12] code C_{70} can be found for $\Omega = \{1, 2, 3, 4, 5, 27, 28\}$. G_{70} is the generator matrix of C_{70} and the weight distribution of C_{70} is given in Table 1. It follows from Table 1 that the weight enumerator of C_{70} is (1) with $\beta = 416$ and $\gamma = 1$.

The existence of a singly-even self-dual [70, 35, 12] code was a open question in [3]. Sloane [12] and Scharlau [11] have indicated in private communications that the first singly-even self-dual [70, 35, 12] code was found by D. Schomaker, but this result was not published. In fact, no self-dual [70, 35, $d \geq 12$] code appears in the literature, so that the code C_{70} is the first published example. Since the largest possible minimum weight is 14, C_{70} is not extremal; however, C_{70} has the largest minimum weight among all known self-dual codes of length 70 and is a 5-error-correcting self-dual code. In [3], Conway and Sloane determined all lengths for which there exist 2-, 3-, and 4-error-correcting self-dual codes. Moreover, all lengths except 62 and 70 were determined for 5-error-correcting codes. This construction method may be used to construct an extremal singly-even [62, 31, 12] code from known codes of length 60. Some inequivalent extremal singly-even [60, 30, 12] codes were found in [3, 7, 8].

3. EXTREMAL FORMALLY SELF-DUAL EVEN CODES

This section considers the existence of some formally self-dual even codes which are not self-dual. Recently, Kennedy and Pless [5] studied formally self-dual even codes, and they also presented methods for constructing

$$G_{70} = \begin{bmatrix}
10 & 11111000000000000000000000011000000 & 11111111111111111111111111111111 \\
00 & 10000000000000000000000000000000000 & 00000111110101110010001000010111111 \\
00 & 01000000000000000000000000000000000 & 10000011111010111001000100001011111 \\
00 & 00100000000000000000000000000000000 & 11000001111101011100100010000101111 \\
00 & 00010000000000000000000000000000000 & 11100000111110101110010001000010111 \\
00 & 00001000000000000000000000000000000 & 11110000011111010111001000100001011 \\
11 & 00000100000000000000000000000000000 & 11111000001111101011100100010000101 \\
11 & 00000010000000000000000000000000000 & 01111100000111110101110010001000010 \\
11 & 00000001000000000000000000000000000 & 10111110000011111010111001000100001 \\
11 & 00000000100000000000000000000000000 & 01011111000001111101011100100010000 \\
11 & 00000000010000000000000000000000000 & 00101111100000111110101110010001000 \\
11 & 00000000001000000000000000000000000 & 00010111110000011111010111001000100 \\
11 & 00000000000100000000000000000000000 & 00001011111000001111101011100100010 \\
11 & 00000000000010000000000000000000000 & 00000101111100000111110101110010001 \\
11 & 00000000000001000000000000000000000 & 10000010111110000011111010111001000 \\
11 & 00000000000000100000000000000000000 & 01000001011111000001111101011100100 \\
11 & 00000000000000010000000000000000000 & 00100000101111100000111110101110010 \\
11 & 00000000000000001000000000000000000 & 00010000101111100000111110101110001 \\
11 & 00000000000000000100000000000000000 & 10001000010111110000011111010111000 \\
11 & 00000000000000000010000000000000000 & 01000100001011111000001111101011100 \\
11 & 00000000000000000001000000000000000 & 00100010000101111100000111110101110 \\
11 & 00000000000000000000100000000000000 & 00010001000010111110000011111010111 \\
11 & 00000000000000000000010000000000000 & 10010001000010111110000011111010111 \\
11 & 00000000000000000000001000000000000 & 11001000100001011111000001111101011 \\
11 & 00000000000000000000000100000000000 & 11100100010000101111100000111110101 \\
11 & 00000000000000000000000010000000000 & 01110010001000010111110000011111010 \\
11 & 00000000000000000000000001000000000 & 10111001000100001011111000001111101 \\
11 & 00000000000000000000000000100000000 & 01011100100010000101111100000111110 \\
11 & 00000000000000000000000000010000000 & 10101110010001000010111110000011111 \\
00 & 00000000000000000000000000001000000 & 11010111001000100001011111000001111 \\
00 & 00000000000000000000000000000100000 & 11101011100100010000101111100000111 \\
11 & 00000000000000000000000000000010000 & 11110101110010001000010111110000011 \\
11 & 00000000000000000000000000000001000 & 11111010111001000100001011111000001 \\
11 & 00000000000000000000000000000000100 & 11111101011100100010000101111100000 \\
11 & 00000000000000000000000000000000010 & 01111101011100100010000101111100000 \\
11 & 00000000000000000000000000000000001 & 00111110101110010001000010111110000 \\
11 & 00000000000000000000000000000000000 & 00011111010111001000100001011111000 \\
11 & 00000000000000000000000000000000000 & 00001111101011100100010000101111100
\end{bmatrix}$$

formally self-dual even codes. In this note, a new method to construct formally self-dual even codes is given.

PROPOSITION 3. *Let A be an n by n $(1, 0)$-matrix such that the numbers of* 1*'s in all rows and columns are odd. If there exist permutation matrices P and Q such that $A^T = PAQ$ where A^T is the transpose of A. Then the following matrix*

$$[I_n, A],$$

generates a formally self-dual even code C.

Proof. Since the number of 1's in each row of A is odd, C is an even code. The matrix $[I_n, A^T]$ generates the code C' which is equivalent to $C^\perp$. Since it holds that $A^T = PAQ$, C and C' are equivalent. Thus C is a formally self-dual even code. ■

A few infinite families of formally self-dual even codes were given in [5]. Any even code with generator matrix of the form $[I_n, B]$, where B is an n by n symmetric matrix and pure and bordered double circulant even codes (see, e.g., [3, 5, 8, 9] for the constructions) are formally self-dual even codes. It is easy to see that the generator matrices of these codes satisfy the assumptions of Proposition 3.

The following corollary describes the construction of a formally self-dual even code from a self-dual symmetric design.

COROLLARY 4. *Let M be an incidence matrix of a self-dual symmetric 2-(v, k, λ) design.*

(i) *If k is odd, the code generated by the matrix $[I_v, M]$ is a formally self-dual even code of length $2v$. Moreover, the minimum weight of this code is at least 4 if $k \geq 3$.*

(ii) *If k is even, the code generated by the matrix*

$$\begin{bmatrix} & \delta & 1 & \cdots & 1 \\ & 1 & & & \\ I_{v+1} & \vdots & & M & \\ & 1 & & & \end{bmatrix},$$

is a formally self-dual even code of length $2v + 2$, where $\delta = ((-1)^v + 1)/2$. Moreover, the minimum weight of this code is at least 4 if $v \geq 3$.

Proof. Since the design is self-dual, the resulting code is a formally self-dual even code in both cases. It is now shown that the minimum weight of the code is at least 4 in both cases. The weight of a sum of two rows of an incidence matrix of a symmetric design is $2(k - \lambda) \geq 2$. Thus the weight of a sum of two rows of the generator matrix is at least 4 in both cases. ■

This is then a family of formally self-dual even $[2v, v, d \geq 4]$ codes constructed from self-dual symmetric designs. The smallest nontrivial symmetric design with respect to the number of blocks is a 2-(7, 3, 1) design. Since any two symmetric 2-(7, 3, 1) designs are isomorphic, this design is self-dual. Using Corollary 4, an extremal formally self-dual even [14, 7, 4] code C_{14} is constructed from this design.

Kennedy and Pless [5] state that the existence of extremal formally self-dual even codes of lengths 36, 38, 44, 46, and 54 is an open question. There cannot exist linear codes with parameters [36, 18, 10] and [44, 22, 12] according to the table of Brouwer and Verhoeff [1]. Thus there is no extremal formally self-dual even code of lengths 36 and 44. The existence

TABLE 2
Near-Extremal Formally Self-Dual Even Codes

Code	$2n$	n	d	Construction	First row
C_{24}	24	12	6	Bordered	01100000011
C_{26}	26	13	6	Pure	1110100001011
C_{32}	32	16	8	Bordered	010111100111101
C_{34}	34	17	8	Pure	11100010000100011
C_{36}	36	18	8	Bordered	01111101001011111

of extremal formally self-dual codes is still unknown for lengths 38, 46, and 54.

The existence of formally self-dual even $[2n, n, 2[n/4]]$ codes is now considered, since there exists no extremal formally self-dual even codes for $2n > 54$. We say that a formally self-dual even $[2n, n, 2[n/4]]$ code is *near-extremal*. Using Corollary 4, a formally self-dual even code C_{16} of length 16 can be constructed from an incidence matrix of a symmetric 2-(7, 4, 2) design, which is a complementary design of a 2-(7, 3, 1) design. Since there exists no extremal formally self-dual even code of length 16, C_{16} is a near-extremal code. Moreover, near-extremal formally self-dual even codes have been found for lengths 24, 26, 32, 34, and 36 using the pure and bordered double circulant constructions. For each code, the parameters, the first row, and the construction are given in Table 2. Note that a formally self-dual even [34, 17, 8] code is not extremal, but the minimum weight of this code is larger than that for self-dual codes of the same length.

Table 2 establishes the largest minimum weight of formally self-dual even codes of length up to 36.

THEOREM 5. *The largest minimum weight of any formally self-dual even code which is not self-dual is known for length* $2n \leq 36$.

TABLE 3
The Largest Minimum Weight of Formally Self-Dual Even Codes but Not Self-Dual

$2n$	d	Codes	Ref.	$2n$	d	Codes	Ref.
6	2	2	[5]	22	6	≥ 2	[5]
8	2	≥ 3	[5]	24	6	≥ 1	C_{24}
10	4	1	[5]	26	6	≥ 1	C_{26}
12	4	≥ 1	[5]	28	8	≥ 1	[15, 5]
14	4	≥ 3	[5], C_{14}	30	8	≥ 1	[5]
16	4	≥ 1	C_{16}	32	8	≥ 1	C_{32}
18	6	1	[5]	34	8	≥ 1	C_{34}
20	6	≥ 1	[5]	36	8	≥ 1	C_{36}

Remark. The actual values are given in Table 3. The third and seventh columns give the number of known codes with the indicated minimum weight and the fourth and eighth columns give the references for the codes.

ACKNOWLEDGMENTS

The author thanks his adviser Professor Hitoshi Kaneta for his helpful discussions and encouragement and Professor T. Aaron Gulliver for his helpful advice after reading the original draft and encouragement. The author also thanks Professor Winfried Scharlau and Professor Neil J. A. Sloane for the information [11, 12] on Schomaker's code.

REFERENCES

1. A. E. Brouwer and T. Verhoeff, An updated table of minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Theory* **39** (1993), 662–677.
2. R. A. Brualdi and V. S. Pless, Weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **37** (1991), 1222–1225.
3. J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.
4. S. T. Dougherty and M. Harada, Extremal doubly-even self-dual codes of length a multiple of 24, submitted.
5. G. T. Kennedy and V. Pless, On designs and formally self-dual codes, *Des. Codes Cryptogr.* **4** (1994), 43–55.
6. G. T. Kennedy and V. Pless, A coding theoretic approach to extending designs, *Discrete Math.* **142** (1995), 155–168.
7. T. A. Gulliver and M. Harada, Weight enumerators of extremal singly-even [60, 30, 12] codes, *IEEE Trans. Inform. Theory* **42** (1996), 658–659.
8. M. Harada, T. A. Gulliver, and H. Kaneta, Classification of extremal double circulant self-dual codes of length up to 62, submitted.
9. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
10. C. L. Mallows and N. J. A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.
11. W. Scharlau, Private communication, December 7, 1995.
12. N. J. A. Sloane, Private communication, November 23, 1995.
13. V. D. Tonchev, "Combinatorial Configurations," Wiley, New York, 1988.
14. H.-P. Tsai, Existence of some extremal self-dual codes, *IEEE Trans. Inform. Theory* **38** (1992), 1829–1833.
15. H. N. Ward, A restriction on the weight enumerator of a self-dual code, *J. Combin. Theory Ser. A* **21** (1976), 253–255.